OPERATIONS SECURITY
PRE-DEPLOYMENT TRAINING

Mandatory IAW USFK Regulation 350-2
and CFC Publication 3-4.9

CFC/USFK CJ39 – IO Division
DSN 723-2149 - OPSEC@Korea.Army.Mil

Overview

- OPSEC Defined
- Critical Information
- Threat & Vulnerability
- OPSEC Responsibilities
- Contact Information

What is OPSEC?

OPERATIONS SECURITY

Denying information to adversaries about our capabilities and intentions by protecting the planning and execution of sensitive activities and operations

---

The Bottom Line:

Keeping our sensitive information out of the hands of the enemy!

OPSEC is a DoD Priority

"…Ensure we are not aiding our enemies by posting content that could put the lives and missions of American Forces and those of our friends and Allies at risk."

- Mr. Donald Rumsfeld, Former Secretary of Defense

"OPSEC is the responsibility of each individual in this Department. To deny our adversaries the opportunity to gather information on our plans, operations, and programs remains a core mission…"

- Mr. Gordon England, Deputy Secretary of Defense

"OPSEC Violations needlessly place lives at risk and degrade the effectiveness of our operations."

- General Peter Schoomaker, Army Chief of Staff

OPSEC is a DoD Priority

"As our AF has become increasingly reliant on advances in information technology for critical mission processes, the importance of OPSEC will increase as we discover new vulnerabilities and work to reduce them."

- General T. Michael Moseley, Air Force Chief of Staff

"Our enemies have proven time and time again their ability to effectively take advantage of lessons learned. We do not need to provide them the means to enhance their capabilities. We need to be Quiet Professionals and protect those things that allow us to succeed on the battlefield. I expect us to hold people accountable that place others at risk."

- General Bryan Brown, CDR Special Operations

OPSEC is a CFC Priority

"Our successful enforcement of OPSEC procedures will prevent serious injury and possibly death of USFK service members…"

"We must make OPSEC a priority and integrate OPSEC practices into our daily activities."

- GEN B.B. Bell, Commander, UNC/CFC/USFK

Critical Information

- Critical Information – Our friendly information that an adversary needs to gain an advantage

- Sensitive, but Unclassified

- **Everyone's responsibility to protect**

"Critical information is listed in the OPSEC portion of an operation plan or order." Joint Pub 3-13.1

CFC Critical Information List

- General Officer/VIP Movement (itineraries, schedules, travel plans)
- Exercise Activities, Scenarios, Events, and Results
- Force Composition; Unit Movement and Locations
- Logistics Caches or Resupply Movement and Locations
- Presence/Employment of New/Improved Technology
- CFC Vulnerabilities and Weaknesses
- Estimates in the Effectiveness of Operations
- Intelligence Capabilities/Purposes/Intent
- Comms Equipment & Procedures: ID/PASSWORDS, Frequencies, Callsigns
- Personal Info: SSN, Financial, Legal, Family, etc

The Threat

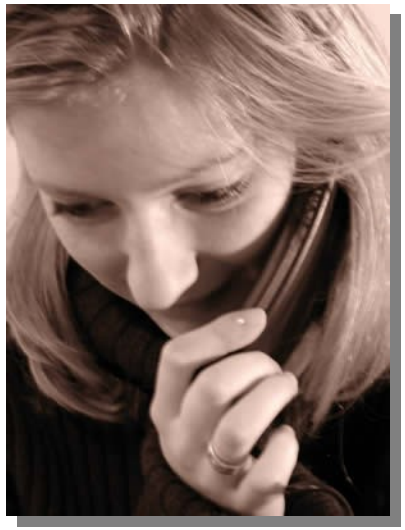
- The Threat is REAL!
- Never underestimate the collect capabilities of an adversary
- Common Means of Collection
  - HUMINT (eavesdropping, dumpster diving, solicitation)
  - SIGINT (telephone, cellular, radio collection)
  - IMINT (satellite, airborne, handheld photography)
  - Open Sources (newspapers, official and personal websites, blogs)
  - Computer Network Operations

Common Vulnerabilities

- **Poor communications practices**
  - Telephone, cellular, email, radio usage
- **Poor computer practices**
  - "easy to hack" or shared passwords
  - Official & Personal Homepages
  - Unauthorized software and
- **Paper disposal**
  - Not destroying sensitive information
- **Shop talk in open / public areas**
- **Family & Friends**

Common Vulnerabilities - Telephone

We're moving out tomorrow. They're not gonna know what hit 'em…



Common Vulnerabilities - Email

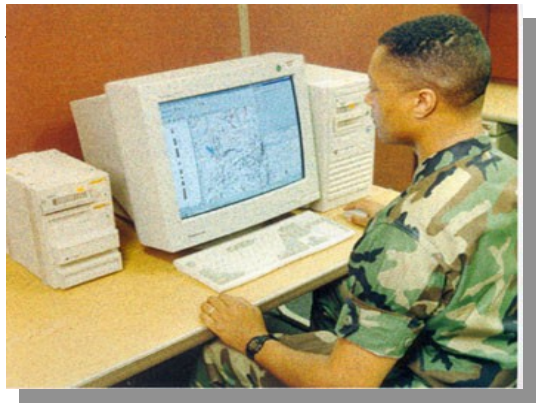
?

?

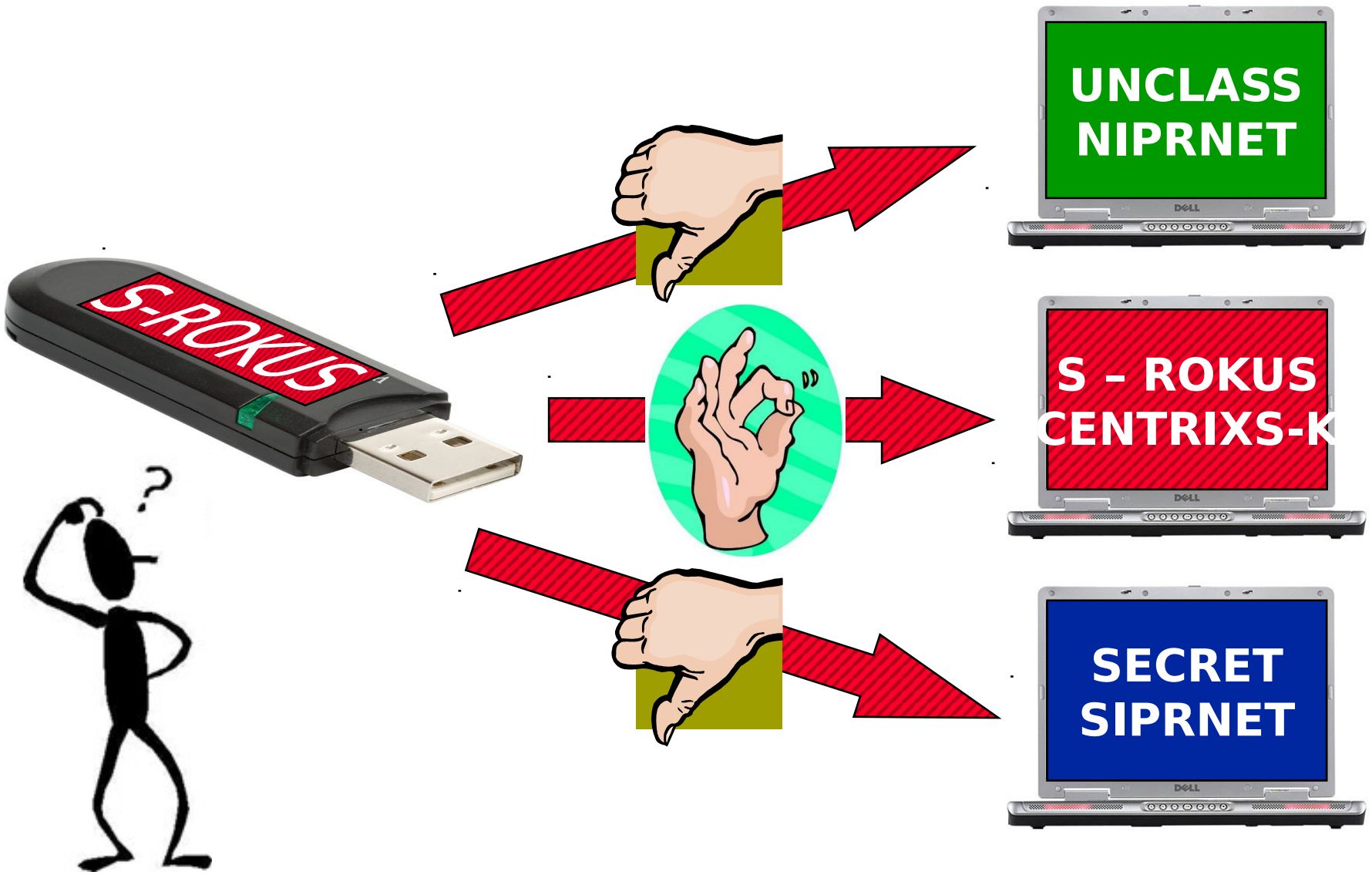
?

INTERNE
T

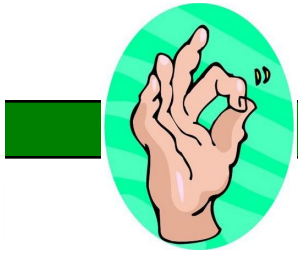
Personal e-mail account

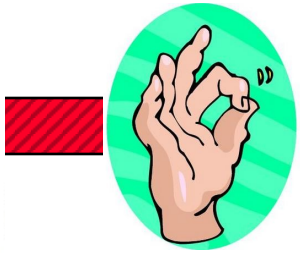


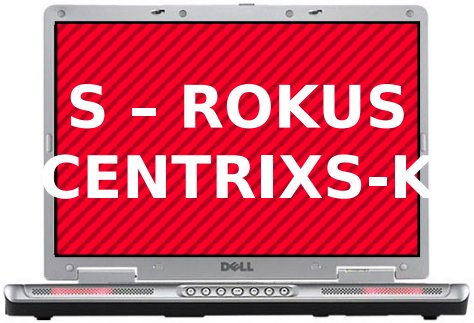
Common Vulnerabilities - USB Drives

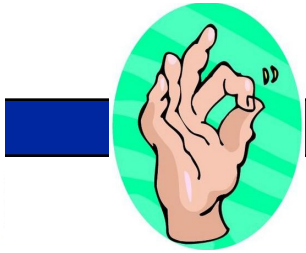


Common Vulnerabilities - USB Drives









Communications Monitor

USFK official telephone calls and emails are monitored for Classified and Critical Information disclosures!

Use of official DoD telecommunications systems constitutes consent to monitoring at all times. DODD 4640.6

AX, MODEM, COMPUTER, INTERNET, LAN/WAN, TELEPHONE
CELLULAR & IRIDIUM PHONE, RADIO, COPIER, PAGER

Apply OPSEC Measures

- Know CFC and unit critical information
- Shred documents containing work or personal information
- Use STU-III / STE when discussing critical information
  - If you're not sure... go secure
  - Don't try to "talk around" classified or sensitive information
- Practice strict phone discipline
  - Halt side conversations if there is an open line nearby
  - Announce "phone up / phone down"
- Do not email critical information over the NIPRNET
  - Use secure network or encrypt using CAC Card
- No sensitive discussions in public places

Apply OPSEC Measures

- And finally, always be aware of your surroundings
  - Immediately report suspicious persons, contacts, or activities

SAEDA Hotline	723-3299
CID (USA-Yongsan)	724-6695
AFOSI (USAF-Osan)	784-1852
NCIS (USN-Yongsan)	723 2467
Military Police (Yongsan)	724-8179
Security Forces (Osan)	784-4350
CFC/USFK OPSEC	723-2149
8th US Army OPSEC	723 4065
CNFK OPSEC	723-6784
7th Air Force OPSEC	784-9788